Government Information Security and Implementation of FISMA

Statement of

Thomas P. Hughes
Chief Information Officer
of the
Social Security Administration

Before the
Committee on Government Reform

March 16, 2006

Cleveland, Ohio

Statement of Thomas P. Hughes
Chief Information Officer
# of the
Social Security Administration
Before the
Committee on Government Reform
March 16, 2006

Mr. Chairman and Members of the Committee, thank you for inviting me here today to discuss government information security at the Social Security Administration (SSA). Commissioner Barnhart, the executives at the agency and I place the highest importance on our information security program and are committed to securing and protecting Federal information. As SSA's Chief Information Officer (CIO), I appreciate the opportunity to discuss our implementation of the Federal Information Security Management Act of 2002 (FISMA).

SSA recognizes the importance of protecting the security and privacy of the people we serve and ensuring the integrity and accuracy of the records we maintain. The Social Security Board's first regulation, published in 1937, dealt with the confidentiality of SSA records. For more than 70 years, since long before the advent of computers and the technology age, SSA has honored its commitment to the American people in maintaining the confidentiality of our records. Our emphasis on privacy has led to a strong commitment in information security.

While we have always safeguarded our records, we also work continuously to ensure that our information technology programs remain responsive to evolving advancements, conditions, and security vulnerabilities. SSA uses a variety of proactive security measures plus independent testing and evaluation of security controls to protect the information that the American public entrusts with us.

Today, as I discuss SSA's compliance with FISMA, and the areas in which we have made significant improvements as well as the areas in which we strive to improve, I am confident you will understand the care I must take in any discussion of the technical details of our specific security processes in a public forum.

Background on FISMA at SSA

The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, or FISMA, requires each Federal agency head to be responsible for security issues including:

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information collected or maintained by or on behalf of the agency
- Complying with the requirements of FISMA and related policies, procedures, standards and guidelines
- Ensuring that information security management processes are integrated with agency strategic and operational planning processes
- Ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control
- Delegating to the agency Chief Information Officer (CIO) the authority to ensure compliance with FISMA including the development of an agency-wide information security program
- Reporting annually to Congress the adequacy and effectiveness of the information security policies, procedures and practices as well as compliance with FISMA

FISMA, along with the Clinger-Cohen Act of 1996 and the Paperwork Reduction Act of 1995, explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, the Office of Management and Budget (OMB), through Appendix III of Circular A-130, requires executive agencies within the federal government to:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibility;
- Periodically review the security controls in their information systems; and
- Authorize system processing prior to operations and, periodically, thereafter.

The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security, or security commensurate with risk, including consideration of the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

SSA takes its responsibility in meeting the requirements of FISMA very seriously. As the Chief Information Officer, I am directly responsible to the Commissioner for ensuring under FISMA that the IT resources of the Agency are adequately secured. The FISMA Certification and Accreditation (C&A) processes provide me, as CIO, and other senior agency officials, with a current picture on the security status of SSA’s 20 major IT systems. All of these systems are important to the performance of our mission. These information systems allow us to run disability processes, recover overpayments, maintain audit trails, track our human resources, and maintain numerous information databases.

We take an agency-wide approach to information technology security at SSA. The CIO and the agency's Deputy Commissioners for Operations, Disability Income Security Programs, Systems, Human Resources, and Finance, Assessment and Management share the accountability for the FISMA C&A process for the major IT systems. In addition, the OCIO works collaboratively with all agency level organizations to ensure that our IT assets are adequately secured.

FISMA Compliance at SSA

SSA uses the FISMA reporting process as an important indicator of how the agency's information technology assets and resources are being protected. Here are the major highlights of the agency's report for FY 05:

Major Systems: SSA has a total of 20 Agency Major Information Systems. All 20 of these systems are currently certified and accredited. In addition, SSA's contingency plan and security controls were tested for each system in the past year.

NIST Security Standards and Guidance: Under FISMA, OMB and the National Institute of Standards and Technology (NIST) develop guidance and standards for Agency systems and security programs. NIST security controls are incorporated into our System Development Life Cycle process. SSA uses special automated software tools to support security self-assessments required by FISMA. These tools also allow us to track any security weaknesses identified.

Incident Detection: SSA follows documented policies and procedures for identifying and reporting incidents of security weakness and uses a combination of automated tools, system monitoring tools and network-penetration type reviews to protect all 20 of our information systems. As required by NIST, SSA provides monthly incident reports to the US Computer Emergency Readiness Team.

Training: SSA provided IT security awareness training to all of our employees (including contractors) and specialized in depth training for those with significant IT security responsibilities. Contractors are required to possess security credentials, expertise and training appropriate to the functions they will be performing before they are permitted to perform services under a contract.

Configuration Management: SSA has an agency wide security configuration policy which is updated as needed to reflect changes in computing platform and in security configuration. All of the operating systems software used at SSA (Windows, Solaris and UNIX, HP, etc) have security configuration policies implemented.

SSA submitted its report for FY 2005 to OMB on October 7, 2005. In March of 2006, OMB provided a combined Federal Agencies FISMA Report which was submitted to Congress.

SSA Office of Inspector General (OIG) FISMA Report

In the second part of the agency's annual FISMA report to OMB, SSA's OIG independently evaluates SSA's information security program and practices. In the FY 2005 report, the OIG determined that SSA met the requirements of FISMA, pointing out that "SSA continues to work towards maintaining a secure environment for its information and systems and has made improvements over the past year to further strengthen its compliance with FISMA". The OIG confirmed that SSA's remediation, certification and accreditation, and inventory processes are sound and made a number of recommendations for improvement:

- *Fully comply with the Agency's risk models and configuration guides*. In response to the recommendation to fully comply with risk models and configuration guides, SSA has developed security documents for every Enterprise Architecture platform in the Agency and expanded this initiative into the database environment as well. We have also developed a cyclical update process for all risk models and configuration guides. We strive to evaluate our architecture for documented mitigations against the latest risks.

  Equally important, the Agency has implemented a monitoring program for each system configuration standard and risk model. This monitoring program provides an accurate and quantifiable picture of the current compliance levels and helps us to meet our FISMA reporting requirements.

- Ensure that the Continuity of Operations Plan (COOP) is updated and tested appropriately. We agree that SSA needs to make sure that both COOP and the Disaster Recovery Plan are updated regularly so that SSA can function in the event of an emergency or disaster. SSA has a schedule for the annual review and update of the COOP plans at the Agency and component levels. The review and update process is conducted in cycles, with the result that updating and testing of the SSA COOP happens on a continuing basis.

  In addition, SSA participated in "exercise Pinnacle," the government-wide COOP exercise last year. This summer, we will participate in "Forward Challenge 06". These exercises validate key elements of the SSA COOP Plan.

  As noted in the OIG's report, the Disaster Recovery Exercise (DRE) was postponed with the concurrence of the OIG and its auditors. The Agency completed its DRE exercise in January 2006. The 2 week exercise was expanded to include more systems and computing platforms along with additional contractors involved with the testing effort.

- *Improve monitoring of contractor security awareness training*. To respond to this recommendation, SSA is implementing a process where all contractors with systems access will complete a security awareness training module. This module provides direct links to current security awareness policy documents as the trainee goes through the program. The trainee is given positive reinforcement through automated responses to answers in the module. The module also allows the agency to monitor the training process and gives an accurate total of trainees who have taken the module.

Other Issues

In the letter of invitation from the Committee, SSA was asked to describe how the Agency identifies and tracks information technology security weaknesses. SSA has established a formal process to track, monitor and resolve weaknesses identified through the FISMA reporting process. SSA is using an automated software tool that allows us to follow corrective security actions through to completion. In addition, the tool produces reports which then allow management to better evaluate the security status of their systems. Other Federal agencies, such as the Environmental Protection Agency, are also using this tool to track, monitor and resolve IT security weaknesses.

The Committee also asked about guidance, resources, and / or procedures agencies need to comply with FISMA. I believe that agencies need to constantly challenge the traditional ‘status quo’. This is critical in any security environment. To be responsive to evolving advancements, conditions, and vulnerabilities, agencies must acknowledge the requirement to continue to improve systems information security on a day-to-day basis. Leadership is also very important. Agencies must have leaders that truly understand today’s security challenges and have the vision to imagine challenges of the future.

Conclusion

Mr. Chairman, Commissioner Barnhart and I, along with all of the senior executives at the Social Security Administration, recognize that information technology systems security is an ongoing challenge and critical component of our mission. While we plan on further improvements with our FISMA reporting in the coming year, we also recognize that FISMA compliance is just one mechanism for security analysis and reporting. Additional and regular internal information technology security evaluations and improvements are also critical pieces to further maintain effective security. We must be vigilant in every way to assure that an individual’s personal information remains secure, taxpayer dollars are protected, and that public confidence in Social Security is maintained. We look forward to working with the Committee to assure the American people that we are doing all we can to maintain the security of the information entrusted to us. Thank you for the opportunity to speak before this committee and I am happy to answer any questions.